RedMimicry is a **semi-automated solution for emulating cyberattacks**. It enables you to test cyber defense measures against realistic scenarios that mimic current threats.

The RedMimicry solution offers a variety of scenarios, **ranging from malware to targeted attacks**, based on the latest tactics and techniques. Through a user-friendly web interface, you can configure and control all scenarios. This significantly reduces the otherwise high manual effort required for realistic emulation of attacker activities.

Areas of Application

RedMimicry is designed for companies that support end customers in **elevating their cyber defense capabilities** and processes. RedMimicry can be used both to validate existing capabilities and processes and in a training context. Through **Purple Teaming** with RedMimicry, the performance of cyber defense measures is efficiently tested and improved by step-wise execution of various attack scenarios and observation of the visibility and response measures.

Instead of only testing isolated attack steps, RedMimicry allows you to emulate **multi-stage and complex threats**. RedMimicry replicates relevant techniques, tactics, and procedures (TTPs) as well as the malware used by real cyber actors, such as the Lockbit group. In our implementation, we ensure that the details relevant to the detection and response to the simulated threat are accurately reproduced. The components used in RedMimicry playbooks are implemented to be **safely deployed in production** networks.

The execution of attacks can be carried out step by step, allowing you to check visibility in monitoring systems, such as **EDR and SIEM**, after each step. Alternatively, the entire attack chain can be executed automatically. Most playbooks also allow you to manually interact with the target system, execute your own commands, or load additional tools. An interactive shell is implemented for this purpose.

RedMimicry GmbH focuses on the continuous development of the platform and playbooks. However, **support during the initial scenarios** and training on the system are possible and advised.

Benefits

Comprehensive: Providers of Red and Purple Teaming services often rely on custom solutions that combine open-source components with frameworks like CobaltStrike, Nighthawk, and Brute Ratel C4. However, these solutions are often difficult to maintain and document, leading to resource conflicts and limiting the quality and quantity of available scenarios. In contrast, RedMimicry offers a library of realistic scenarios that encompass complete attack chains.

Repeatable: With RedMimicry, you require minimal effort to test additional endpoints or repeat previous tests.

User-Friendly: Unlike custom solutions, RedMimicry's user interface is accessible to less experienced users and well-documented. Even junior staff can launch and orchestrate complex attacks with just a few clicks.

Frequent Updates: RedMimicry provides updates for existing playbooks and continuously develops new scenarios. This ensures that the executed attacks always reflect the current threat landscape.

Data Privacy: You can use RedMimicry as on-premises software. In this case, no end customer data is transmitted to RedMimicry GmbH, and you retain full control over ongoing scenarios. This facilitates the use of RedMimicry even in companies with high data protection requirements.

Contact

RedMimicry GmbH
Mahlower Straße 24
12049 Berlin
Germany

Stefan Steinberg
Chief Operating Officer
stefan.steinberg@redmimicry.com
+49 155 60175358